EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S33	87359	(tugenberg near steven) (hardy near douglas) (tkasik near thomas) motorola	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/31 12:15
S34	446	S33 and (secur$3 near2 memory)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/31 12:17
S35	169	S34 and (memory same key same process$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/31 12:17
S36	27	S35 and (gate same logic$5)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/31 12:19
S37	1	S36 and (laser adj scrib$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/05/31 12:21

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L6	508	713/194	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 12:52
L7	40	6 and (process$3 same memory same key same logic)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:05
L8	42	6 and (process$3 same memory same key and gate)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:06
L9	16	7 and gate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 12:57
L10	16	9 and 8	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 12:58
L11	42	9 8	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 12:58
L12	13	8 and (secure near2 memory)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:00
L14	42268	"713"/$.ccls. "380"/$.ccls. "726"/$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:01
L15	2757	14 and ((process$3 memory) near2 secure)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:03

EAST Search History

L16	3887	14 and ((process$3 memory) near2 (secure protected tamper))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:04
L17	164	16 and ((block$3 logic) near2 gate)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:05
L18	32	17 and (process$3 same memory same key same logic)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:05
L19	32	18 and (process$3 same memory same key and gate)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 15:06

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L20	83372	(block$3 logic) near2 gate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 17:41
L21	8000	20 and (logic near circuitry)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 17:42
L22	37	21 and ((process$3 memory) near2 secure)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 17:43
L23	18	22 and (process$3 same memory same key and gate)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 17:43
L24	5	22 and (process$3 same memory same key same logic)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 17:44

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L25	0	(process$4 and secure and (storage medium media disk$4 CD) and logic and memory and (laser-scribed laser-ascribed laser) and circuit$4 and encrypt$4 and key and gate and (data information content document$5 text plaintext) and (bus network$3 link connect$3 LAN WAN)).CLM.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/01 18:51

Terms used **encryption key logic circuitry secure memory blocking gates**

Found **8** of **177,263**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 8 of 8

Relevance scale

1 Key management for encrypted broadcast

Avishai Wool
May 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 2
Publisher: ACM Press
Full text available: pdf(220.36 KB) Additional Information: full citation, abstract, references, index terms

We consider broadcast applications where the transmissions need to be encrypted, such as direct broadcast digital TV networks or Internet multicast. In these applications the number of encrypted TV programs may be very large, but the secure memory capacity at the set-top terminals (STT) is severely limited due to the need to withstand pirate attacks and hardware tampering. Despite this, we would like to allow the service provider to offer different packages of programs to the users. A user ...

Keywords: conditional access, pay-per-view

2 Key management for encrypted broadcast

Avishai Wool
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

3 DRM experience: Digital rights management in a 3G mobile phone and beyond

Thomas S. Messerges, Ezzat A. Dabbish
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(306.59 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed

and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

4 Performance Considerations for an Embedded Implementation of OMA DRM 2

Daniel Thull, Roberto Sannino

March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**

Publisher: IEEE Computer Society

Full text available: pdf(139.35 KB) Additional Information: full citation, abstract, citings

As digital content services gain importance in the mobile world, Digital Rights Management (DRM) applications will become a key component of mobile terminals. This paper examines the effect dedicated hardware macros for specific cryptographic functions have on the performance of a mobile terminal that supports version 2 of the open standard for Digital Rights Management defined by the Open Mobile Alliance (OMA). Following a general description of the standard, the paper contains a detailed analy ...

Keywords: DRM, Security, Mobile Terminal, Cryptography

5 Architecture for Protecting Critical Secrets in Microprocessors

Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhenghong Wang

May 2005 **ACM SIGARCH Computer Architecture News , Proceedings of the 32nd Annual International Symposium on Computer Architecture ISCA '05**, Volume 33 Issue 2

Publisher: IEEE Computer Society, ACM Press

Full text available: pdf(143.62 KB) Additional Information: full citation, abstract, index terms

We propose "secret-protected (SP)" architecture to enable secure and convenient protection of critical secrets for a given user in an on-line environment. Keys are examples of critical secrets, and key protection and management is a fundamental problem ⁉ often assumed but not solved ⁉ underlying the use of cryptographic protection of sensitive files, messages, data and programs. SP-processors contain a minimalist set of architectural features that can be built into a general-purpose microprocess ...

6 Key management for restricted multicast using broadcast encryption

Michel Abdalla, Yuval Shavitt, Avishai Wool

August 2000 **IEEE/ACM Transactions on Networking (TON)**, Volume 8 Issue 4

Publisher: IEEE Press

Full text available: pdf(291.54 KB) Additional Information: full citation, references, citings, index terms, review

7 Virtual machine monitors: Implementing an untrusted operating system on trusted hardware

David Lie, Chandramohan A. Thekkath, Mark Horowitz

October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Publisher: ACM Press

Full text available: pdf(280.87 KB) Additional Information: full citation, abstract, references, citings, index terms

Recently, there has been considerable interest in providing "trusted computing platforms" using hardware~---~TCPA and Palladium being the most publicly visible examples. In this paper we discuss our experience with building such a platform using a traditional time-sharing operating system executing on XOM~---~a processor architecture that provides copy protection and tamper-resistance functions. In XOM, only the processor is trusted; main memory and the operating system are not trusted.Our opera ...

Keywords: XOM, XOMOS, untrusted operating systems

8 Efficient Memory Integrity Verification and Encryption for Secure Processors

G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas

December 2003 **Proceedings of the 36th annual IEEE/ACM International Symposium on Microarchitecture**

Publisher: IEEE Computer Society

Full text available: pdf(307.01 KB) Additional Information: full citation, abstract, citings, index terms

Secure processors enable new sets of applications suchas commercial grid computing, software copy-protection,and secure mobile agents by providing security from bothphysical and software attacks. This paper proposes newhardware mechanisms for memory integrity verification andencryption, which are two key primitives required in single-chipsecure processors. The integrity verification mechanismoffers significant performance advantages over existingones when the checks are infrequent as in grid com ...

Results 1 - 8 of 8